

REMARKS

Claims 1-37, 42, 43, 47, 52, and 53 are currently pending in the application. Claims 1-37, 42, 43, 47, 52, and 53 stand rejected.

The Examiner rejected claims 1-14, 18-32, 36, 37, and 47 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,082,532 (Vick). The Examiner also rejected claims 15-17, 42, 43, 33-35, 52, and 53 under 35 U.S.C. 103(a) as being unpatentable over Vick as applied to claims 1, 19, 37, and 47 in view of U.S. Patent No. 6,493,758 (McLain). The rejections are respectfully traversed.

Vick describes techniques “for providing distributed web server authentication of users.” See Summary of the Invention. “[W]hen a user attempts to access a web server in an authentication ring, the web server requests a user ID cookie and a credential cookie from the user.” See column 3, lines 34-36. “The “User ID Cookie” contains the user ID for the user. The “Credential Cookie” contains the information needed to certify that the user is who the user claims to be.” See column 3, lines 46-49. “If the user doesn't have a valid credential cookie for the site,...the user is redirected to a LOGON page where the user's user ID and password must be re-entered....The web server authenticates the entered user ID and password pair against a local authentication mechanism, for example, an operating system. If the user ID and password are authenticated, the web server creates an encrypted password cookie containing user information selected from, for example, the user's user ID and password, IP address and a time stamp, and where the encryption is performed using a secret key known only to those web servers participating in the authentication ring. A “time stamp” specifies the date and time that the password cookie was created or last updated. Each time the user hits a new web server, the new web server updates the time stamp in the password cookie.” See column 3, line 51 to column 4, line 1. “Since the credentials (user ID and password), of the current user can be automatically retrieved from the user by the server at any time, it is unnecessary to request that

the user re-enter the user ID and password credentials each time the user attempts to connect to a different server.” See column 4, lines 10-15. Vick’s technique enables “both individual and related local and remote web sites to implement user authentication without waiting for a fully functional certificate technology to emerge. Additionally, embodiments of the present invention will enhance and simplify the user’s experience with the web site. In another embodiment, the present invention is used in virtual private web rings to give the user the appearance of a single log-in across multiple sites. “Virtual Private Web Rings” are a federated group of sites which support the same cookie key.” See column 4, lines 16-25. As will be discussed, Vick does not teach or suggest several important limitations contained in the claims of the present application.

Claim 1 of the present application is directed to “[a]n interoperability system for providing access to a plurality of services by a plurality of users.” “[T]he plurality of services [are] associated with and controlled by a plurality of independent service providers and employing a plurality of interfaces at least some of which are not directly interoperable.” The Examiner referred to column 6, lines 40-50, as describing the interfaces which “are not directly interoperable.” The Applicants respectfully disagree.

The passage to which the Examiner referred is part of a description of the flow diagram of Fig. 5 relating to how a user accesses web pages “that are located at separate web sites.” Column 5, lines 59-60. Column 6, lines 20-40 describe how a user accessing web pages on web site A can subsequently access web pages on web site B using Vick’s technique, i.e., by using the encrypted password cookie (obtained by web site B from web site A) and the private key. Lines 40-50 of column 6 specifically describe how, if the password cookie has expired or is no longer valid, web site B requires the user to re-enter his user ID and password to establish an authenticated session. At no place does Vick suggest that web sites A and B employ “interfaces ...which are not directly interoperable.” To the contrary, Vick indicates that web sites A and B can readily communicate with each other to facilitate the hand off of the user from the first site to

the second. See, for example, column 6, lines 28-31, in which the request to connect the user to web site B is sent to web site B from web site A. If Vick taught interfaces which were not directly interoperable, more would be needed to enable such a request. Because Vick makes no mention of what might be required, the necessary inference is that web sites A and B *are* directly interoperable.

The interoperability system recited in claim 1 includes “at least one data store having a directory stored therein which maps an identity corresponding to each of the users to a policy framework which defines access policies relating to the services.” “[E]ach of the plurality of users [is] associated with one of a plurality of independent enterprises,” and “the identity for each user” stored in the directory “identify[ies] the associated enterprise.” The Examiner pointed to column 3, lines 50-67, and column 4, lines 15-25, as describing the recited directory and the policy framework to which user identities are mapped. The Applicants respectfully disagree.

As an initial matter, Vick does not teach or suggest that users are from different enterprises or that a user identity stored in a directory identifies an associated enterprise. The only reference to different enterprises in Vick relates to the operators of the web sites to which user access is being facilitated. No references are made to an enterprise with which the user himself is associated, or whether such an association is stored in a directory.

In addition, and as discussed above, column 3, lines 50-67, and column 4, lines 15-25, of Vick are part of a general description of the manner in which Vick employs an encrypted password cookie and private key “to give the user the appearance of a single log-in across multiple sites,” i.e., “a federated group of sites which support the same cookie key.” Column 4, lines 23-25. Vick does not teach or suggest “a policy framework which defines access policies relating to the services” or a directory “which maps an identity corresponding to each of the users to [the] policy framework.” Column 3, lines 50-67, merely describes standard authentication with a user ID and password. No policy framework is mentioned, particularly not

one to which user identities (that include references to “one of a plurality of independent enterprises”) are mapped.

Claim 1 recites that the system’s data store(s) also include(s) “a plurality of rich client objects...operable to be launched within browser environments on the client machines, and to interact with the services via the interoperability system.” The Examiner referred to references to standard HTML web pages in Vick as anticipating the “rich client objects” recited in claim 1. The Applicants respectfully disagree.

As discussed in the previous response, and as described in the present application, a rich client is “a software application or applet (or a collection of such software objects) which is operable to be launched in a browser on a client machine. A rich client typically includes both the display logic which governs what is displayed on the client machine, as well as some level of application logic (i.e., executable code) which provides functionality on the client machine which, in the past, has typically been provided by code on the remote server.” Rich client technology is employed by embodiments of the present invention “to provide access to application services in an even more flexible and efficient manner.” See paragraphs [0086] and [0087] of the present application. As would be understood by those of skill in the art, rich clients are readily distinguishable from the standard web pages to which Vick refers in a number of respects. That is, as is well known, web pages are structured documents encoded using hypertext markup language (HTML) which may be retrieved from remote web sites and viewed in a client browser. Web pages may include images, text, hyperlinks to other documents, etc. By contrast, a rich client includes “some level of application logic (i.e., executable code) which provides functionality on the client machine,” and, as recited in claim 1 is operable “to interact with the services via the interoperability system.” The standard web pages referred to in Vick are not characterized by such capabilities.

The system recited in claim 1 also includes “at least one computing device which is

operable to...selectively facilitate interaction among the uploaded rich client objects and the services with reference to the directory and the policy framework.” The Examiner points to the same passages in columns 3 and 4 discussed above to anticipate this functionality of the recited computing device(s). The Applicants respectfully disagree with the Examiner’s assertion.

As discussed above, Vick does not teach or suggest the claimed directory or policy framework, or the storage or use of rich clients recited in claim 1. Neither does Vick teach or suggest that users might be of different enterprises, or that this might be reflected in such a directory and/or policy framework. It therefore follows that Vick does not teach or suggest any functionality of one or more computing devices that involves the uploading of rich client objects to user devices, and facilitation of “interaction among the uploaded rich client objects and the services with reference to the directory and the policy framework.” Rather, Vick describes a mechanism by which a user may sign in with a user ID and password once, and then view pages from different web sites without having to repeat the sign in process too often. Vick simply does not have the capability of “enabling...users associated with different...enterprises to independently access [a] plurality of services” in the manner enabled by the interoperability system recited in claim 1 of the present application.

In view of the fact that Vick does not teach or suggest several important limitations recited in claim 1, the rejection of claim 1 over Vick should be withdrawn. In addition, the rejection of claims 2-37, 42, 43, 47, 52, and 53 should also be withdrawn for at least the reasons discussed.

//

//

//

//

//

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested. If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at (510) 663-1100.

Respectfully submitted,
WEAVER AUSTIN VILLENEUVE & SAMPSON LLP

/Joseph M. Villeneuve/

Joseph M. Villeneuve
Reg. No. 37,460

P.O. Box 70250
Oakland, California 94612-0250
(510) 663-1100